



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/895,344	06/29/2001	Avraham Mualem	42390P11391	6903

8791 7590 06/28/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER

SHIFERAW, ELENI A

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 06/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/895,344

Applicant(s)

MUALEM ET AL.

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 April 2005.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-45 is/are pending in the application.
4a) Of the above claim(s) 42 is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 1-41, and 43-45 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Final Rejection

Response to Amendment

1. Applicant's arguments/amendments with respect to canceled claim 42, amended claims 1, 11, 21, 31, 41, and 43, filed on April 14, 2005 have been fully considered but they are not persuasive. The examiner would like to point out that this action is made final (MPEP 706.07a).

Response to Arguments

2. Applicant argues that:

- a. Independent claims 1, 11, and 21 are not taught by Anand to include "*a metric value associated with a security association*" (page 10 last paragraph).
- b. The references, whether alone or in combination, fail to support "*associating a metric value with a security association of a traffic stream and modifying the metric value based on network traffic generated for the traffic stream*" (page 11 first and last paragraph, page 12 last paragraph, and page 13 par. 2).
- c. *Dependent claims 2-10, 12-20, 22-30, 32-40, and 43-45 are allowable based upon their dependency on allowable claims 1, 11, 21, 31, and 41 (page 12 par. 2, and page 13 par. 2).*

However, Examiner disagrees with applicant.

Regarding argument (a), Argument is not persuasive. Anand teaches associating a metric value with a security association by determining the metric value (the heaviness or intensiveness of encryption/decryption process) and associating the metric value with security association (performing encryption/decryption in NIC) (Anand page 2 par. 0014 and 0015).

Regarding argument (b), Argument is not persuasive. Klincewicz discloses modifying the metric value (link lengths) of a network traffic based on the value and weighted sum value of link lengths, and routing the traffic according to the shortest paths with respect to link lengths (Klincewicz col. 6 lines 30-58).

Regarding argument (c), examiner disagrees with applicant. Based on the arguments set forth by the examiner for arguments (a) and (b), the dependent claims stand rejected.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. Therefore, the examiner asserts that the system of the prior art, Anand and Klincewicz do teach or suggest the subject matter as recited in independent claims 1, 11, 21, 31, and 41. Dependent claims 2-10, 12-20, 22-30, 32-40, and 43-45 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action dated April 14, 2005. Accordingly, rejections for claims 1-41, and 43-45 are respectfully maintained.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1-4, 7-14, 17-24, 27-34, and 37-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anand et al. (Anand, Pub. No US 2002/0062333A1) in view of Klincewicz et al. (Klincewicz, Patent No.: US 6,697,334 A1).

As per claims 1, 21, and 31 Anand teaches a method/medium comprising:

associating a security association with a traffic stream (Anand Page 2 par. 0017;
associating an encryption/decryption with data packet traffic stream);

associating a metric value with the security association (Anand Page 2 par. 0014; metric value of encryption/decryption is heavy or intensive so cryptography is performed in NIC); and

dynamically mapping the traffic stream to one of multiple components that perform cryptography operations based on the metric value (Anand Page 2 par. 0014 and 0015;
dynamically mapping tasks to components that perform cryptography operations (intensive tasks are mapped to NIC or less intensive tasks are mapped to Host CPU) to eliminate multiple CPU cycles to host).

Anand do not explicitly teach modifying the metric value based on an amount of network traffic generated for the traffic stream.

Klincewicz teaches modifying the metric value based on network traffic (Klincewicz Col. 5 lines 23-53; modifying the metrics of message sizes within the traffic stream);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Klincewicz within the system of Anand because it would determine if eliminating and/or adding any given link would improve the cost, or other relevant metric, of the network (Klincewicz col. 1 lines 51-55).

As per claim 11 Anand teaches an apparatus comprising:

a network interface coupled to receive network traffic streams (Anand Fig. 2 No. 126);
and

a driver agent coupled to communicate with the network interface (Anand Fig. 2 No. 116, 118, & 120), the driver agent to associate a security association with a traffic stream (Anand Page 2 par. 0017; associating an encryption/decryption with data packet traffic stream), associate a metric value with the security association (Anand Page 2 par. 0014; metric value of encryption/decryption is heavy or intensive so cryptography is performed in NIC), and dynamically map the traffic stream to one of multiple components that perform cryptography operations based on the metric value (intensive tasks are mapped to NIC or less intensive tasks are mapped to Host CPU) to eliminate multiple CPU cycles to host).

Anand do not explicitly teach modifying the metric value of the security association based on how much network traffic is received for the traffic stream.

Klincewicz teaches modifying the metric value based on network traffic (Klincewicz Col. 5 lines 23-53; modifying the metrics of message sizes within the traffic stream);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Klincewicz within the system of Anand because it would determine if eliminating and/or adding any given link would improve the cost, or other relevant metric, of the network (Klincewicz col. 1 lines 51-55).

As per claims 2, 12, 22, and 32 Anand teaches the method wherein the dynamic mapping is performed using a time-based analysis (Anand page 2 par. 0017).

As per claims 3, 13, 23, and 33, both Anand and Klincewicz teach the subject matter as described above. In addition, Anand teaches the method wherein the multiple components comprise a driver agent and a network interface (Anand page 5 par. 0038, 0045 and page 2 par. 0014; Host and NIC).

As per claims 4, 14, 24, and 34, both Anand and Klincewicz teach the subject matter as described above. In addition, Anand teaches the method wherein dynamically mapping traffic streams to one of multiple components comprises selecting between performing cryptography operations with a driver agent and performing cryptography operations with a network interface using cached cryptography information (Anand Page 2 par. 0014 and 0015).

As per claims 7, 17, 27, and 37 both Anand and Klincewicz teach the subject matter as described above. In addition, Anand teaches the method wherein modifying the metric value further comprises initializing the metric to a predetermined value when the security association is received by a driver agent (Anand Fig. 5 No. 304).

As per claims 8, 18, 28, and 38 both Anand and Klincewicz teach the subject matter as described above. In addition, Klincewicz teaches the method wherein modifying the metric value further comprises changing the associated metric value by a predetermined amount when the security association is added to a cache (Klincewicz Col. 5 lines 22-53; modifying link metrics when traffic stream that has cryptography information is added). The rationale for combining are the same as claim 1 above.

As per claims 9, 19, 29, and 39 both Anand and Klincewicz teach the subject matter as described above. In addition, Klincewicz teaches the method wherein modifying the metric value further comprises changing the associated metric value when a packet is received (Klincewicz Col. 5 lines 22-53; modifying link metrics value when traffic stream when the packet is received). The rationale for combining are the same as claim 1 above.

As per claims 10, 20, 30, and 40 both Anand and Klincewicz teach the subject matter as described above. In addition, Klincewicz teaches the method wherein modifying the metric value

further comprises periodically changing the metric value independent of network traffic (Klincewicz Col. 5 lines 22-53). The rationale for combining are the same as claim 1 above.

5. Claims 5-6, 15-16, 25-26, 36-36, 41 and 43-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anand et al. (Anand, Pub. No US 2002/0062333A1) in view of Klincewicz et al. (Klincewicz, Patent No.: US 6,697,334 A1) and Mitchem et al. (Mitchem, Patent No.: US 6,209,101 B1).

As per claim 41 Anand teaches a method comprising:

associating a security association with a traffic stream (Anand Page 2 par. 0017;
associating an encryption/decryption with data packet traffic stream);

associating a metric value with a security association (Anand Page 2 par. 0014; metric value of encryption/decryption is heavy or intensive so cryptography is performed in NIC);

initializing the metric value to a predetermined value when the security association is received by a driver agent (Anand col. 5 lines 54-65);

Anand do not explicitly teach modifying the metric value based on an amount of network traffic generated for the traffic stream.

Klincewicz teaches modifying the metric value based on network traffic (Klincewicz Col. 5 lines 23-53; modifying the metrics of message sizes within the traffic stream);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Klincewicz within the system of Anand

because it would determine if eliminating and/or adding any given link would improve the cost, or other relevant metric, of the network (Klincewicz col. 1 lines 51-55).

Anand and Klincewicz fail to explicitly teach determining whether the security association necessary for performing cryptography operations on a packet of the traffic stream is cached;

determining whether the security association should be cached based on the metric value; and

caching the security association if it is determined from the metric value that the security association should be cached.

However Mitchem discloses determining whether the security association necessary for performing cryptography operations on a packet of the traffic stream is cached (Mitchem Col. 5 lines 65-col. 6 lines 18; determining whether the security association necessary for performing cryptography operations should be cashed in order reload the new security associations when organization root policy/metric value changes);

determining whether the security association should be cached based on the metric value (Mitchem Col. 5 lines 65-col. 6 lines 18; determining whether the security association should be cashed based on previous policy/metric value); and

caching the security association if it is determined from the metric value that the security association should be cached (Mitchem Col. 5 lines 65-col. 6 lines 18).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Mitchem within the combination system of Anand and Klincewicz because it would provide adaptive security system which can readily adjust to organizational policy changes and dynamically implement new security policies (Mitchem col. 1 lines 27-49). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made employ the teachings of Mitchem within Anand and Klincewicz and determine whether the security association necessary for performing cryptography operations on the packet should be cached based on the predetermined policy, and caching the security association if it is determined from the predetermined policy because it would decide to handle one network traffic stream with Inline Operation (NIC) and another network traffic stream with the Secondary Use model (host).

As per claims 5, 15, 25, and 35 both Anand and Klincewicz teach all the subject matter as described above. In addition Anand discloses dynamically mapping when the metric value is greater or when intensive operation is required (Anand page 2 par. 0014).

Anand and Klincewicz do not explicitly teach wherein dynamically mapping comprises replacing a cached security association with a non-cached security.

However Mitchem teaches the method wherein the dynamic mapping further comprises replacing a cached security association with a non-cached security association (Mitchem Col. 5 lines 65-col. 6 lines 18) that reads on the method wherein the dynamic mapping further comprises replacing a cached security association with a non-cached security association when

the metric value of the non-cached security association is greater than (differs) from the metric value of the cached security association by at least a predetermined amount.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Mitchem within the system of Anand and Klincewicz because it would provide adaptive security system which can readily adjust to organizational policy changes and dynamically implement new security policies (Mitchem col. 1 lines 27-49). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made employ the teachings of Mitchem within Anand and Klincewicz and determine whether the security association necessary for performing cryptography operations on the packet should be cached based on the predetermined policy, and caching the security association if it is determined from the predetermined policy because it would decide to handle one network traffic stream with Inline Operation (NIC) and another network traffic stream with the Secondary Use model (host).

As per claims 6, 16, 26, and 36 Anand, Klincewicz, and Mitchem teach the subject matter as described above. In addition, Klincewicz teaches the method wherein the predetermined amount is selected based on a cost-based analysis (Klincewicz Abstract). The rationale for combining are the same as claim 1 above.

As per claim 43, Anand, Klincewicz, and Mitchem teach the subject matter as described above. In addition, Anand teaches the method wherein the determining whether the security association should be cached further comprises:

determining whether the metric value is greater than the lowest metric value of security associations by at least a predetermined amount (Anand Page 2 par. 0014; metric value is determined and mapped to NIC when intensive operation and mapped to host when lesser operation).

increasing the value of the metric value by a predetermined amount when the associated security association is added to a cache (Klincewicz col. 5 lines 23-53);

incrementing the value of the metric value when a packet for the associated traffic stream is received (Klincewicz col. 5 lines 23-53); The rational for combining are the same as claim 1 above.

As per claim 44, Anand, Klincewicz, and Mitchem teach the subject matter as described above. In addition, Anand teaches the method further comprising periodically decreasing the metric value (Anand page 2 par. 0014; packet is mapped to NIC or host and metric value is periodically decreased).

As per claim 45, Anand, Klincewicz, and Mitchem teach all the subject matter as described above. In addition, the combinations of the prior art teach the method further comprising periodically evaluating the metric value to determine whether the security association should be cached (Anand col. 6 lines 30-44, and Mitchem col. 5 lines 65-col. 6 lines 27).

Conclusion

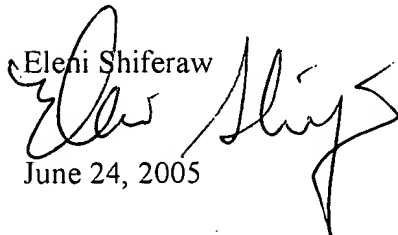
6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw

June 24, 2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100